This book presents an up-to-date, unified treatment of research in bounded arithmetic and complexity of propositional logic with emphasis on independence proofs and lower bound proofs. The author discusses the deep connections between logic and complexity theory and lists a number of intriguing open problems.

An introduction to the basics of logic and complexity theory is followed by discussion of important results in propositional proof systems and systems of bounded arithmetic. Then more advanced topics are treated, including polynomial simulations and conservativity results, various witnessing theorems, the translation of bounded formulas (and their proofs) into propositional ones, the method of random partial restrictions and its applications, direct independence proofs, complete systems of partial relations, lower bounds to the size of constant-depth propositional proofs, the method of Boolean valuations, the issue of hard tautologies and optimal proof systems, combinatorics and complexity theory within bounded arithmetic, and relations to complexity issues of predicate calculus.

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

EDITED BY G.-C. ROTA

Volume 60

Bounded Arithmetic, Propositional Logic, and Complexity Theory

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

4 W. Miller, Jr. *Symmetry and separation of variables*
6 H. Minc *Permanents*
11 W. B. Jones and W. J. Thron *Continued fractions*
12 N. F. G. Martin and J. W. England *Mathematical theory of entropy*
18 H. O. Fattorini *The Cauchy problem*
19 G. G. Lorentz, K. Jetter, and S. D. Riemenschneider *Birkhoff interpolation*
21 W. T. Tutte *Graph theory*
22 J. R. Bastida *Field extensions and Galois theory*
23 J. R. Cannon *The one-dimensional heat equation*
25 A. Salomaa *Computation and automata*
26 N. White (ed.) *Theory of matroids*
27 N. H. Bingham, C. M. Goldie, and J. L. Teugels *Regular variation*
28 P. P. Petrushev and V. A. Popov *Rational approximation of real functions*
29 N. White (ed.) *Combinatorial geometries*
30 M. Pohst and H. Zassenhaus *Algorithmic algebraic number theory*
31 J. Aczel and J. Dhombres *Functional equations containing several variables*
32 M. Kuczma, B. Chozewski, and R. Ger *Iterative functional equations*
33 R. V. Ambartzumian *Factorization calculus and geometric probability*
34 G. Gripenberg, S.-O. Londen, and O. Staffans *Volterra integral and functional equations*
35 G. Gasper and M. Rahman *Basic hypergeometric series*
36 E. Torgersen *Comparison of statistical experiments*
37 A. Neumaier *Interval methods for systems of equations*
38 N. Korneichuk *Exact constants in approximation theory*
39 R. A. Brualdi and H. J. Ryser *Combinatorial matrix theory*
40 N. White (ed.) *Matroid applications*
41 S. Sakai *Operator algebras in dynamical systems*
42 W. Hodges *Model theory*
43 H. Stahl and V. Totik *General orthogonal polynomials*
44 R. Schneider *Convex bodies*
45 G. Da Prato and J. Zabczyk *Stochastic equations in infinite dimensions*
46 A. Bjorner, M. Las Vergnas, B. Sturmfels, N. White, and G. Ziegler *Oriented matroids*
47 G. A. Edgar and L. Sucheston *Stopping times and directed processes*
48 C. Sims *Computation with finitely presented groups*
49 T. Palmer *Banach algebras and the general theory of *-algebras*
50 F. Borceux *Handbook of Categorical Algebra I*
51 F. Borceux *Handbook of Categorical Algebra II*
52 F. Borceux *Handbook of Categorical Algebra III*
54 A. Katok and B. Hasselblatt *Introduction to the modern theory of dynamical systems*
58 R. Gardner *Geometric tomography*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Bounded Arithmetic, Propositional Logic, and Complexity Theory

JAN KRAJÍČEK
Academy of Sciences of the Czech Republic

CAMBRIDGE UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1995

Library of Congress Cataloging-in-Publication Data

Krajíček, Jan.

Bounded arithmetic, propositional logic, and complexity theory / Jan Krajíček.

p. cm. – (Encyclopedia of mathematics and its applications; v. 60)

Includes bibliographical references (p. 000–000) and indexes.

ISBN 0-521-45205-8

1. Constructive mathematics. 2. Proposition (Logic).
3. Computational complexity. I. Title. II. Series.
QA9.56.K73 1995

511.3 – dc20 94-47054
CIP

A catalog record for this book is available from the British Library.

ISBN 0-521-45205-8 hardback

Transferred to digital printing 2004

To Karel Tesař

CONTENTS

PREFACE

The central problem of complexity theory is the relation of deterministic and nondeterministic computations: whether P equals NP, and generally whether the polynomial time hierarchy PH collapses. The famous *P versus NP problem* is often regarded as one of the most important and beautiful open problems in contemporary mathematics, even by nonspecialists (see, for example, Smale [1992]).

The central problem of bounded arithmetic is whether it is a finitely axiomatizable theory. That amounts to deciding whether there is a model of the theory in which the polynomial time hierarchy does not collapse.

The central problem of propositional logic is whether there is a proof system in which every tautology has a proof of size polynomial in the size of the tautology. In this generality the question is equivalent to asking whether the class NP is closed under complementation. Particular cases of the problem, to establish lower bounds for usual calculi, are analogous to constructing models of associated systems of bounded arithmetic in which $\mathrm{NP} \neq \mathrm{coNP}$.

Notions, problems, and results about complexity (of predicates, functions, proofs, ...) are deep-rooted in mathematical logic, and (good) theorems about them are among the most profound results in the field. Bounded arithmetic and propositional logic are closely interrelated and have several explicit and implicit connections to the computational complexity theory around the P versus NP problem. Central computational notions (Turing machine, Boolean circuit) are crucial in the metamathematics of the logical systems, and models of these systems are natural structures for concepts of computational complexity.

Moreover, the only approach in sight universal enough to have a chance of producing lower bounds to the size of general Boolean circuits needed for the first problem is the method of approximations, which is a version of the ultraproduct construction (and of forcing); forcing bears a relation to the second and the third problems, and a general framework for the last problem is in terms of Boolean valuations (Sections 3.1, 9.4, 12.7, and 13.3).

Much of the contemporary research in computational complexity theory concentrates on proving weaker versions of P $\neq$ NP, for example, on proving lower bounds to the size of restricted models of circuits, and some deep results (although telling little about the P versus NP problem) have been obtained.

It is, however, possible to approach the same problem differently and to try to prove statement P $\neq$ NP first for other structures than natural numbers $\boldsymbol{N}$, in particular for nonstandard models of systems of bounded arithmetic.

Such an approach is, in fact, common in mathematics, where for example a number-theoretic conjecture about the field of rational numbers is first tested for function fields that share many properties with the rationals. Similarly, we can try to prove that P $\neq$ NP holds in a model of a system of bounded arithmetic. Nonstandard models of systems of bounded arithmetic are not ridiculously pathological structures, and a part of the difficulty in constructing them stems exactly from the fact that it is hard to distinguish these structures, by the studied properties, from natural numbers.

Methods (all essentially combinatorial) used for known circuit lower bounds are demonstrably inadequate for the general problem. It is to be expected that a nontrivial combinatorial or algebraic argument will be required for the solution of the P versus NP problem. However, I believe that the close relations of this problem to bounded arithmetic and propositional logic indicate that such a solution should also require a nontrivial insight into logic. For example, recent strong lower bounds for constant-depth proof systems needed a reinterpretation of logical validity (Section 12.4).

The relations among bounded arithmetic, propositional logic, and complexity theory are not ad hoc but are reflected in numerous more specific relations, ranging from intertranslatability of arithmetic and propositional proofs and computations of machines, to characterizations of provably total functions in various subsystems of bounded arithmetic in terms of familiar computational models, correspondence in definability of predicates by restricted means and their decidability in a particular computational model, to proof methods based on analogous combinatorial backgrounds in all three areas, and finally to formalizability of basic concepts and methods of complexity theory within bounded arithmetic. It is the main aim of this book to explain these relations.

The last several years have seen important developments in areas of complexity theory, as well as in bounded arithmetic and complexity of propositional logic, and other deep relations between these areas have been established. Although there are several monographs on computational complexity theory and very good survey articles covering the main fields of research, many recent results in bounded arithmetic and propositional logic are scattered in research articles, and some important facts, such as relations between various theorems and methods, are only a part of unpublished folklore or appeared in a longer but now less significant, and hence less read, work.

To my knowledge there are three published monographs treating, at least partially, bounded arithmetic and its relation to complexity theory: Wilkie (1985), Buss (1986), and the last part of Hájek and Pudlák (1993) (Chapter 5, pp. 267–408). Although these are very interesting books, the first two contain none of the developments of the last several years (obviously) and none of the three treats propositional logic.

This book is not intended to be a textbook of either logic or complexity theory. It merely wants to present the main aspects of contemporary research in bounded arithmetic and complexity of propositional logic in a coherent way and to illustrate topics pointed out at the beginning of this Preface. It is aimed at research mathematicians, computer scientists, and graduate students. No previous knowledge of the topics is required, but it is expected that the reader is willing to learn what is needed along the way. My hope is that the book will stimulate more people to contribute to this fascinating area.

Prague Jan Krajíček
July 28, 1994

ACKNOWLEDGMENTS

I thank my colleagues Petr Hájek, Pavel Pudlák, Jiří Sgall, Antonín Sochor, and Vítězslav Švejdar from our logic seminar at the Mathematical Institute of the Academy of Sciences at Prague for creating an extremely stimulating and encouraging research environment. In particular, I have learned a lot from extensive collaboration with Pavel Pudlák.

I am also indebted to Gaisi Takeuti (Urbana), Sam Buss (San Diego), and Peter Clote (Boston), with whom I had the privilege of collaborating on various research projects. Gaisi Takeuti never failed to provide an inspiration during my two years at the Department of Mathematics of the University of Illinois at Urbana.

I also wish to thank Steve Cook from the Department of Computer Science of the University of Toronto, where I wrote a large part of the first version of this book during my stay in spring semester 1993, for many inspiring discussions concerning topics related to this book.

Finally I thank the following people for comments on parts of the manuscript: M. Baaz (Vienna), S. R. Buss (San Diego), M. Chiari (Parma), S. A. Cook (Toronto), F. Pitt (Toronto), P. Pudlák (Prague), A. A. Razborov (Moscow), G. Takeuti (Urbana), and D. Zambella (Amsterdam).